| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/736,688 | 12/12/2000 | David Michael Kurn | 20206-035 (P00-3417) | 7936 |

7590            12/01/2004

Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

| EXAMINER |
|---|
| JACK, TODD M |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2133 | |

DATE MAILED: 12/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

| | Application No. | Applicant(s) |
|---|---|---|
| **Office Action Summary** | 09/736,688 | KURN ET AL. |
| | **Examiner** | **Art Unit** | |
| | Todd M Jack | 2133 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1) ☒ Responsive to communication(s) filed on <u>*13 July 2004*</u>.

2a) ☒ This action is **FINAL**.    2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4) ☒ Claim(s) *1-7 and 9-16* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-7 and 9-16* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. §§ 119 and 120**

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

13) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application)
since a specific reference was included in the first sentence of the specification or in an Application Data Sheet.
37 CFR 1.78.

    a) ☐ The translation of the foreign language provisional application has been received.

14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific
reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

**Attachment(s)**

| | | | |
|---|---|---|---|
| 1) ☐ Notice of References Cited (PTO-892) | | 4) ☐ Interview Summary (PTO-413) Paper No(s). _____ . |
| 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) | | 5) ☐ Notice of Informal Patent Application (PTO-152) |
| 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ . | | 6) ☒ Other: *Examiner's Statement.* |

## DETAILED ACTION

### *Response to Arguments*

Applicant's arguments filed 07/13/2004 have been fully considered but they are not persuasive.

Claim 1: The applicant argues that Ford and Liao fail to teach that keys held or generated by Ford's key release agent should "authenticate authorizations to access the sensitive information in the database". The examiner finds that Ford teaches a key release agent which authenticates the identity and attributes of the decrypting system. It is inherent in Ford that access to decryption key is denied if appropriate access control criteria is not met.(col. 6, lines 12-18)

The applicant argues that Ford and Liao fail to teach "an agent on the remote server" or "a key repository processor on the central server". The examiner finds that Ford teaches a key release agent distributing a message encryption key through the computer network (col. 4, lines 14-19) and Ford teaches trusted servers called key release agents (col. 3, lines 45-46).

Claim 4: The applicant argues that Ford fails to teach what the relationship should be between the duplicate agents. The examiner finds that Ford teaches trusted servers called key release agents in an application environment were broad user populations have access to encrypted information (col. 3, lines 45-46).

The applicant argues that Ford and Liao fail to teach "where in the agent in the remote server is an independent key repository process". The examiner finds that Ford teaches a broad user populations inherently have access to encrypted information; e.g. File servers (col. 3, lines 49-50).

Claim 7: The applicant argues that Liao and Ford fails to teach that keys held or generated by the key release agent should do anything other than decipher the encrypted message that has traversed a computer network. The examiner finds that Ford teaches to calculate a decryption key and no other entity can modify the access control attributes (col. 6, lines 24-32).

The applicant argues that Ford and Liao fail to teach "one or more master keys for managing information in the database". The examiner finds that Geer teaches a smart card's public key of the user authorize the signature on the ID certificate, thus the public key acts as a master key managing the transactions (col. 3, lines 6-10).

The applicant argues that Ford and Liao fails to teach "establishing communications between the key process and an agent on behalf of the key repository process". The examiner finds that Geer teaches smart card's public key of the user establishes a transaction between the transaction computer and the authorized computer. The smart card acts as an agent for the transaction computer where file servers (i.e. agents) process keys. (col. 2, lines 26-39)

Claim 9:  The applicant argues that Ford and Liao fail to teach "an agent process" and

"a key repository process that controls access to the database".  The examiner finds

that Geer teaches smart card's public key of the user establishes a transaction between

the transaction computer and the authorized computer.  The smart card acts as an

agent for the transaction computer where file servers (i.e. agents) process keys. (col. 2,

lines 26-39)

Claim 11:  The applicant argues that Liao and Ford fails to teach that keys held or

generated by the key release agent should do anything other than decipher the

encrypted message that has traversed a computer network.  The examiner finds that

Ford teaches to calculate a decryption key and no other entity can modify the access

control attributes (col. 6, lines 24-32).

The applicant argues that Ford and Liao fail to teach "an agent on behalf of the key

repository process".  The examiner finds that Geer teaches smart card's public key of

the user establishes a transaction between the transaction computer and the authorized

computer.  The smart card acts as an agent for the transaction computer where file

servers (i.e. agents) process keys. (col. 2, lines 26-39)

The applicant argues that Ford and Liao fail to teach "an agent on the remote server" or

"a key repository processor on the central server".  The examiner finds that Ford

teaches a key release agent distributing a message encryption key through the

computer network (col. 4, lines 14-19) and Ford teaches trusted servers called key

release agents (col. 3, lines 45-46).


Claim 13:  The applicant argues that Liao combined with Ford fails to teach that any

keys held or generated by the key release agent should do anything other than decipher

the cipher text of an encrypted message that has traversed a computer network.  The

examiner finds that Ford teaches where the encrypted message traverses a computer

network from an encryptor to a decryptor (col. 6, lines 20-24).


### Response to Amendment

The claim 8 cancellation filed on 07/13/2004 under 37 CFR 1.131 has been

considered but is ineffective to overcome the Ford, Liao, and Geer references.


### Claim Rejections - 35 USC § 102

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 9-10 are rejected under 35 U.S.C. 102(b) as being anticipated by Ford

(5,481,613).

Claim 9:  Ford teaches a server system in a computer network that results in access

control criteria are reflected in access control attributes which form part of the access

control decryption block.  Decryption keys are delivered when the identity and attributes

of the decrypting system match a set of access control criteria. (col. 6, lines 12-37), a

public file server is connected to a key release agent which is a server system in a

computer (col. 6, lines 4-32), the key release agent which is trusted to deliver decryption

keys to decrypting systems only when the identity and attributes of the decrypting

system match a set of access control criteria (col. 6, lines 12-18) and smart card's

public key of the user establishes a transaction between the transaction computer and

the authorized computer.  The smart card acts as an agent for the transaction computer

where file servers (i.e. agents) process keys. (col. 2, lines 26-39)

Claim 10:  Further, Ford teaches a key release agent can calculate the decryption key

and no other entity can modify the access control attributes in a way which the key

release agent would not detect (col. 6, lines 28-32).

## Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-2, 4-6, and 11-16 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Ford (5,481,613) in view of Liao (6,606,663).

Claim 1:  Ford teaches a key release agent is a server system in a computer network

which is trusted to deliver decryption keys to decrypting systems only when the identity

and attributes of the decrypting system match a set of access control criteria determined

by the encrypting system at the time of encrypting (col. 6, lines 10-18), the form of the

access controlled decryption block is such that only a recognized key release agent can

calculate the decryption key and no other entity can modify the access control attributes

in a way which the key release agent would not detect (col. 6, lines 28-32), and key

release agent is a server system (col. 6, lines 10-18). Ford teaches a key release agent

which authenticates the identity and attributes of the decrypting system. It is inherent in

Ford that access to decryption key is denied if appropriate access control criteria is not

met.(col. 6, lines 12-18). Ford teaches a key release agent distributing a message

encryption key through the computer network (col. 4, lines 14-19) and Ford teaches

trusted servers called key release agents (col. 3, lines 45-46). Ford fails to teach a

central server, a remote server, a database on the central server, enterprise credentials

stored in the database, one application on the remote server, and the agent

authenticates authorizations of specific applications to access resources based upon

authorizations held. Liao teaches web service devices (col. 6, lines 41-42) acting as a

central server, proxy server which refers to a piece of hardware equipment that

comprises one or more microprocessors, memory, buses, and interface (col. 6, lines 43-

45) acting as a remote server, cache of a wireless client's credentials when a credential

is sent to the wireless user agent to a protected Internet server—the proxy server

retrieves the credential from the cache (col. 7, lines 55-67 and col. 8, lines 1-5),

credential is cached in memory (col. 7, lines 61-63), if the wireless client device wishes

to communicate with web server within protected realm, the wireless device must

provide a credential (col. 8, lines 42-44), and a number of services available on the

global Internet require that a user authenticate itself before access to a protected

service (col. 7, lines 41-47). It would have been obvious to a person having ordinary

skill in the art at the time the invention was made to modify Ford's system by including

the servers, database, one application on the server, and where the agent

authenticates. The modifications would have been obvious because a person having

ordinary skill in the art would have been motivated to do so, as suggested by Liao, in

order to control access to the cryptographic/computer system, store sensitive data

obtained on the server for later use, and allow the server to access authorized

resources.


Claim 2: Ford teaches a data structure, which is generated by the encrypting system,

contains a statement of the access control criteria relating to the encryption plus key

related data which will enable a key release agent to calculate the decryption key (col.

6, lines 24-28). Ford teaches an E key is the ACD key or ACD keys may contain the E

key as well as other keys. Each KRA holds each R-key used in its domain. (col. 6, lines

36-42) It can be seen that the key release agent acts as a repository for keys.


Claim 4: Ford teaches a key release agent is a server system in a computer network

which is trusted to deliver decryption keys to decrypting systems only when the identity

and attributes of the decrypting system match a set of access control criteria determined

by the encrypting system at the time of encrypting (col. 6, lines 10-18), trusted servers

called key release agents in an application environment were broad user populations

have access to encrypted information (col. 3, lines 45-46) and a broad user populations

inherently have access to encrypted information; e.g. File servers (col. 3, lines 49-50).

Claim 5: Ford teaches a key-release private key (col. 6, lines 4-20) which acts as a

decryptor, thus protecting the sensitive information.

Claim 6: Ford teaches a key-release private key (col. 6, lines 4-20) which acts as a

decryptor, thus allowing access to only authorized individuals to provide privacy

protection.

Claim 11: Ford teaches a key release agent can calculate the decryption key and no

other entity can modify the access control attributes in a way which the key release

agent would not detect (col. 6, lines 28-32), key release agent which is trusted to deliver

decryption keys to decrypting systems only when the identity and attributes of the

decrypting system match a set of access control criteria (col. 6, lines 12-18), calculate a

decryption key and no other entity can modify the access control attributes (col. 6, lines

24-32) and smart card's public key of the user establishes a transaction between the

transaction computer and the authorized computer. The smart card acts as an agent for

the transaction computer where file servers (i.e. agents) process keys. (col. 2, lines 26-

39). Ford teaches a key release agent distributing a message encryption key through

the computer network (col. 4, lines 14-19) and Ford teaches trusted servers called key

release agents (col. 3, lines 45-46). Ford fails to teach a remote server configured to

communicatively couple to a central server, an application program on the remote

server, and access a cryptographically protected database on the central server. Liao

teaches a web service device acting as a central server connected to a proxy server

(col. 6, lines 41-42), if the wireless client device wishes to communicate with web server

within protected realm, the wireless device must provide a credential (col. 8, lines 42-

44), and the credential is cached in the memory of a proxy server and a number of

services available on the global Internet require that a user authenticate itself before

access to a protected service (col. 7, lines 41-47). It would have been obvious to a

person having ordinary skill in the art at the time the invention was made to modify

Ford's system by including a remote server, application program, and cryptographically

protected database. These modifications would have been obvious because a person

having ordinary skill in the art would have been motivated to do so, as suggested by

Liao, in order to have remote servers located in personal computers distributed widely

to be in contact with a central server distributing information.

Claim 12: Further, Ford teaches a data structure, which is generated by the encrypting

system, contains a statement of the access control criteria relating to the encryption

plus key related data which will enable a key release agent to calculate the decryption

key (col. 6, lines 24-28).

Claim 13: Ford teaches a key release agent is a server system in a computer network

which is trusted to deliver decryption keys to decrypting systems only when the identity

and attributes of the decrypting system match a set of access control criteria determined

by the encrypting system at the time of encrypting (col. 6, lines 10-18) and where the

encrypted message traverses a computer network from an encryptor to a decryptor (col.

6, lines 20-24). Ford fails to teach a central server and a database on the central server

configured to contain sensitive information. Liao teaches web service devices (col. 6,

lines 41-42) acting as a central server and a cache of a wireless client's credentials

when a credential is sent to the wireless user agent to a protected Internet server—the

proxy server retrieves the credential from the cache (col. 7, lines 55-67 and col. 8, lines

1-5). It would have been obvious to a person having ordinary skill in the art at the time

the invention was made to modify Ford's system by including the servers and database.

The modifications would have been obvious because a person having ordinary skill in

the art would have been motivated to do so, as suggested by Liao, in order to control

access to the cryptographic/computer system, store sensitive data obtained on the

server for later use, and allow the server to access authorized resources.

Claim 14: Further, Ford teaches a key release agent is a server system in a computer

network which is trusted to deliver decryption keys to decrypting systems only when the

identity and attributes of the decrypting system match a set of access control criteria

determined by the encrypting system at the time of encrypting (col. 6, lines 10-18).

Claim 15: Further, Ford teaches a key-release private key (col. 6, lines 4-20) which acts

as a decryptor, thus protecting the sensitive information.

Claim 16:  Further, Ford teaches a key-release private key (col. 6, lines 4-20) which acts as a decryptor, thus allowing access to only authorized individuals to provide privacy protection.


Claims 3 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ford in view Liao, further in view of Geer (6,192,131 B1).

Claim 3:  Further, Ford fails to teach the level of trust is defined as the number of individuals required for reconstructing the master key and/or for performing a sensitive operation.  Greer teaches the convener will create a new conversation certificate and distribute it to a new set of parties (col. 11, lines 33-49).  It is seen that the level of trust will be determined by how parties are permitted to participate in the sensitive conversation.  If a portion of the log is found to be super-encrypted, the parties who hold the additional keys could be persuaded to open their sub-conversations using those keys (col. 11, lines 33-38).  It would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Ford's system by including the needed trust of a number of individuals required for reconstructing a key.  The modifications would have been obvious because a person having ordinary skill in the art would have been motivated to do so in order to ensure the sensitive information stored was accessed by an unauthorized individual.

Claim 7: Ford teaches a key-release private key which acts as a decryptor, which is

delivered to decryption keys to decrypting systems only when the identity and attributes

of the decrypting system match a set of access criteria (col. 6, lines 4-20), a key release

agent is a server system in a computer network which is trusted to deliver decryption

keys to decrypting systems only when the identity and attributes of the decrypting

system match a set of access control criteria determined by the encrypting system at

the time of encrypting (col. 6, lines 10-18), a data structure which is generated by the

encrypting system, contains a statement of the access control criteria relating to the

encryption plus key related data which will enable a key release agent to calculate the

decryption key & calculate a decryption key and no other entity can modify the access

control attributes (col. 6, lines 24-32),. Ford fails to teach storing enterprise credentials

in a database on a central server and authenticating by the agent and one or more

master keys for managing the information in the database. Liao teaches the credential

is cached in the memory of a proxy server and a number of services available on the

global Internet require that a user authenticate itself before access to a protected

service (col. 7, lines 41-47). It would have been obvious to a person having ordinary

skill in the art at the time the invention was made to modify Ford's system by including

the storing of credentials in a database and authenticating authorizations of specific

applications on the remote server. This modification would have been obvious because

a person having ordinary skill in the art would have been motivated to do so, as

suggested by Liao, in order that sensitive credentials are protected from unauthorized

access. Further, Greer teaches a private key of the identification certificate for the smart

card at the authorizing computer acts as the authorizing agent (col. 3, lines 3-10) and

Geer teaches a smart card's public key of the user authorize the signature on the ID

certificate, thus the public key acts as a master key managing the transactions (col. 3,

lines 6-10), smart card's public key of the user establishes a transaction between the

transaction computer and the authorized computer. The smart card acts as an agent for

the transaction computer where file servers (i.e. agents) process keys. (col. 2, lines 26-

39). It would have been obvious to a person having ordinary skill in the art at the time

the invention was made to modify Ford's system by including the master keys for

managing the information in the database. This modification would have been obvious

because a person having ordinary skill in the art would have been motivated to do so,

as suggested by Greer, in order that the database can be secured and open to only

authorized individuals.

### *Conclusion*

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Todd M Jack whose telephone number is 571-272-3823. The examiner can normally be reached on M-Fridays.
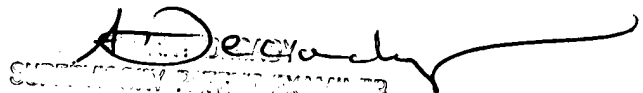
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on 571-272-3819. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Todd Jack
Art unit 2133

November 09, 2004